IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

WENDY BRYAN and PATRICIA WHITE, individually and on behalf of all others similarly situated, Plaintiffs, v. BioPlus Specialty Pharmacy Services, LLC, Defendant.	)	**Case No.:** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Wendy Bryan and Patricia White ("Plaintiffs"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby allege the following against Defendant BioPlus Specialty Pharmacy Services, LLC ("BioPlus" or "Defendant").

NATURE OF THE ACTION

1. This is a class action for damages with respect to BioPlus Specialty Pharmacy Services, LLC, for its failure to exercise reasonable care in securing and safeguarding its patients' sensitive personal data—including names, addresses, email addresses, dates of birth, Social Security numbers, health insurance billing

information, and treating physician information, collectively known as Personally Identifiable Information ("PII" or "Private Information").

2. This class action is brought on behalf of patients whose sensitive PII was stolen by cybercriminals in a cyber-attack that accessed sensitive patient information through BioPlus's services on or around October 25, 2021 (the "Data Breach").

3. The Data Breach affected at least 350,000 individuals from BioPlus's services.

4. BioPlus reported to Plaintiffs that information compromised in the Data Breach included their PII.

5. Plaintiffs were not notified until December of 2021, nearly three months after their information was first accessed.

6. As a result of the Data Breach, Plaintiffs and other Class Members will experience various types of misuse of their PII in the coming years, including but not limited to unauthorized credit card charges, unauthorized access to email accounts, and other fraudulent use of their financial accounts.

7. Defendant's security failures enabled the hackers to steal the Private Information of Plaintiffs and other members of the class—defined below. These failures put Plaintiffs' and other Class Members' Private Information at a serious, immediate, and ongoing risk. Additionally, Defendant's failures caused costs and

expenses associated with the time spent and the loss of productivity from taking time to address and attempt to ameliorate the release of personal data, as well as emotional grief associated with constant monitoring of personal banking and credit accounts. Mitigating and dealing with the actual and future consequences of the Data Breach has also created a number of future consequences for Plaintiffs and Class Members—including, as appropriate, reviewing records of fraudulent charges for services billed but not received, purchasing credit monitoring and identity theft protection services, the imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, the loss of property value of their personal information, and the stress, nuisance, and aggravation of dealing with all issues resulting from the Data Breach.

8. Plaintiffs and Class Members suffered a loss of the property value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of the loss of the property value of personal information in data breach cases.

9. There has been no assurance offered from BioPlus that all personal data or copies of data have been recovered or destroyed. BioPlus offered one free year of Experian IdentityWorks's Credit 3B monitoring services, which does not guarantee the security of Plaintiffs' information. To mitigate further harm, Plaintiffs

chose not to disclose any more information to receive services connected with BioPlus.

10. Accordingly, Plaintiffs assert claims for negligence, breach of contract, breach of implied contract, and breach of fiduciary duty, as well as a claim for declaratory relief.

PARTIES, JURISDICTION, AND VENUE

A. Plaintiff Wendy Bryan

11. Plaintiff Wendy Bryan is a citizen of New Jersey and brings this action in her individual capacity and on behalf of all others similarly situated. Ms. Bryan has resided in the state of New Jersey for nearly fifty years and owns a home within the state. Ms. Bryan intends to remain in New Jersey indefinitely.

12. Ms. Bryan used BioPlus's services in 2021 when she had a specialty prescription filled through her doctor's office. To receive services at BioPlus, Plaintiff Bryan was required to disclose her PII, which was then entered into BioPlus's database and maintained by Defendant. In maintaining her information, Defendant expressly and impliedly promised to safeguard Plaintiff Bryan's PII. Defendant, however, did not take proper care of Ms. Bryan's PII, leading to its exposure as a direct result of Defendant's inadequate security measures. In December of 2021, Plaintiff Bryan received a notification letter from Defendant stating that her sensitive PII was taken.

13. The letter also offered one year of credit monitoring through Experian's IdentityWorks Credit 3B monitoring, which was and continues to be ineffective for Bryan and other Class Members. The Experian credit monitoring would have shared Ms. Bryan's information with third parties and could not guarantee complete privacy of her sensitive PII.

14. In the months and years following the Data Breach, Ms. Bryan and the other Class Members will experience a slew of harms as a result of Defendant's ineffective data security measures. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent.

15. Plaintiff Bryan greatly values her privacy, especially in receiving medical services, and would not have paid the amount that she did for pharmacy services if she had known that her information would be maintained using inadequate data security systems.

B. Plaintiff Patricia White

16. Plaintiff Patricia White is a citizen of Connecticut and brings this action in her individual capacity and on behalf of all others similarly situated. Ms. White has resided in Connecticut for her entire life, has a registered automobile in the state of Connecticut, and has been a member of local civic groups in the state of

Connecticut for nearly three decades. She intends to remain in Connecticut indefinitely.

17. Ms. White's information was entered into BioPlus's systems in 2015 when a clerical error resulted in her prescription information from her doctor's office being sent to BioPlus instead of her in-network pharmacy. Ms. White corrected the clerical error and canceled the service from BioPlus, but her information remained in Defendant's systems, vulnerable to misuse, until the data breach occurred in November of 2021. In maintaining her information within its systems, Defendant expressly and impliedly promised to safeguard Ms. White's PII. Defendant did not properly safeguard, Ms. White's PII, however, resulting in this information being exposed during the data breach. Ms. White received a notice letter from Defendant that her information was taken in December of 2021.

18. The letter also offered two years of Experian IdentityWorks Credit 3B monitoring, which was and continues to be ineffective for Ms. White and the other members of the class. Accepting the credit monitoring from BioPlus would have meant transmitting sensitive PII back to Defendant after they had already demonstrated that they could not be trusted with such information.

19. Some of the damages that will occur with respect to absent Class Members have already manifested themselves In Plaintiff White's experience. Ms. White received a notification from her credit monitoring services through H &R

Block on or about November 30, 2021, that her information appeared on the dark web, where cyber-criminals trade sensitive patient information for use in phone, banking, and health insurance scams. Ms. White has notified her credit monitoring services of this breach and continues to monitor her accounts for suspicious activity.

20. In the months and years following the data breach event, Ms. White and the other Class Members will experience a slew of harms as a result of Defendant's ineffective data security measures. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent.

21. Ms. White values the privacy of her personal information. She would not have agreed to having her information transmitted to BioPlus's systems—even by mistake—if she had known that it would be stored using inadequate storage methods that would lead to its misuse.

C. Defendant BioPlus

22. Defendant BioPlus Specialty Pharmacy Services, LLC, a Florida limited liability company, is a specialty pharmacy company, with its principal place of business located in the State of Florida at 376 Northlake Boulevard, Alamonte Springs, FL 32701. BioPlus conducts business nationally, including in the states of New Jersey and Connecticut. BioPlus offers a number of pharmacy services, including patient and provider pharmaceutical approval, and prescription fill and

refill services. BioPlus registered its headquarters at 376 Northlake Boulevard, Alamonte Springs, FL 32701. BioPlus's corporate policies and practices, including those used for data privacy, are established in, and emanate from, Florida.

23. BioPlus Specialty Pharmacy Services, LLC has two individual members—Stephen Vogt and Stephen Garner, both of whom are residents of Florida and intend to remain in Florida. In addition to two individual members, BioPlus Specialty Pharmacy Services, LLC has one LLC member—BioPlus Parent, LLC, a Rhode Island entity whose sole member, John Figueroa, resides in and intends to remain in Rhode Island. BioPlus Specialty Pharmacy Services, LLC, is therefore a citizen of Rhode Island and Florida.

D. Jurisdiction

24. The Court has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class Members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

25. The Court has personal jurisdiction over Defendant because Defendant's principal place of business is located in this District.

E. Venue

26. Venue is proper in this district under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore

resides in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

FACTS

27. Defendant provides a wide variety of pharmacy services to patients across the country. As part of its business, Defendant was entrusted with, and obligated to safeguard and protect the Private Information of Plaintiffs and the Class in accordance with all applicable laws.

28. In November of 2021, Defendant first learned of an unauthorized entry into its network, which contained customers' Private Information including names, addresses, email addresses, dates of birth, Social Security numbers, financial account numbers, billing, and other health information. Defendant posted the following notice on its website:[1]

> December 10, 2021 — BioPlus Specialty Pharmacy Services, LLC ("BioPlus") is committed to protecting the confidentiality and security of the information we maintain. This notice concerns a data security incident that may have involved some of that information.
>
> On November 11, 2021, we identified suspicious activity in our IT network. Upon learning of the incident, we immediately took steps to isolate and secure our systems. We also launched an investigation with the assistance of a third-party forensic firm and notified law enforcement.

[1] *Update on Cyber Incident*, (Dec. 10, 2021), https://bioplusrx.com/cyber-incident/ [hereinafter *Data Breach Notice*].

> Through the investigation, we determined that an unauthorized party gained access to our IT network between October 25, 2021 and November 11, 2021. During that time, the unauthorized party accessed files that contained information pertaining to certain BioPlus patients. However, our investigation could not rule out the possibility that information pertaining to all current and former BioPlus patients may have been subject to unauthorized access.
>
> On December 10, 2021, we began mailing letters to all current and former patients whose information may have been involved. The information subject to unauthorized access may have included patient names, dates of birth, addresses, medical record numbers, current/former health plan member ID numbers, claims information, diagnoses, and/or prescription information. For certain patients, Social Security numbers were also involved. As a precautionary measure, the letters include guidance on how patients can protect their information. Additionally, for patients whose Social Security number was involved, we are offering complimentary credit monitoring and identity protection services. We have also established a dedicated, toll-free call center for patients to call with questions. If you believe you are affected but do not receive a letter by January 10, 2022, please call 1-855-545-2336, available Monday through Friday, between 9:00 am and 6:30 pm, Eastern Time.
>
> We take this issue very seriously, and deeply regret any concern this incident may have caused. To help prevent something like this from happening again, we have implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor our systems.

29. Upon learning of the Data Breach in November 2021, Defendant investigated. As a result of the Data Breach, Defendant initially estimated that the

Private Information of at least 350,000 patients were potentially compromised stemming from services previously received.[2]

30. In December of 2021 Defendant announced that it first learned of suspicious activity that allowed on ore more cybercriminals to access their systems through a ransomware attack. The 2021 Notice disclosed that a ransomware attack enabled a threat actor to access BioPlus systems.

31. Defendant offered no explanation for the delay between the initial discovery of the Breach and the belated notification to affected customers, which resulted in Plaintiffs and Class Members suffering harm they otherwise could have avoided had a timely disclosure been made.

32. BioPlus's notice of Data Breach was not just untimely but woefully deficient, failing to provide basic details, including but not limited to, how unauthorized parties accessed its networks, what information was accessed, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach occurred system-wide, whether servers storing information were accessed, and how many patients were affected by the Data Breach. Even worse, BioPlus offered only one or two years of identity monitoring

[2] These numbers were reported to the Health and Human Services Healthcare Data Breach Portal. *See Cases Currently Under Investigation*, U.S. DEP'T OF HEALTH & HUMAN SERVS.: BREACH PORTAL, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf [hereinafter *Breach Portal*] (last visited Dec. 28, 2021).

to Plaintiffs and Class Members, which required the disclosure of additional PII that BioPlus had just demonstrated it could not be trusted with.

33. Plaintiffs and Class Members' PII is currently for sale to criminals on the dark web, meaning that unauthorized parties have accessed and viewed Plaintiffs' and Class Members' unencrypted, unredacted information, including names, addresses, email addresses, dates of birth, Social Security numbers, member ID numbers, policyholder names, employer names, policy numbers name, and more.

34. The Breach occurred because Defendant failed to take reasonable measures to protect the PII it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated warnings to the healthcare industry, insurance companies, and associated entities about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on other healthcare providers.

35. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through unauthorized

access by an unknown third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe.

A. Defendant's Privacy Promises

36. BioPlus made, and continues to make, various promises to its customers, including Plaintiffs, that it will maintain the security and privacy of their Private Information.

37. In its Notice of Privacy Practices, Defendant stated the following:

- "We do not give out, exchange, barter, rent, sell, lend, or disseminate to any unauthorized person, any information about patients that is considered patient confidential, is restricted by law, or has been specifically restricted by a patient in a signed HIPAA authorization form"

- "Information about each patient is only used or disclosed as is reasonably necessary to carry out treatment, to obtain payment for treatment, and to conduct health care operations."

38. BioPlus describes how it may use and disclose medical information for each category of uses or disclosures, none of which provide it a right to expose patients' Private Information in the manner it was exposed to unauthorized third parties in the Data Breach.

39. By failing to protect Plaintiffs' and Class Members' Private Information, and by allowing the Data Breach to occur, BioPlus broke these promises to Plaintiffs and Class Members.

B. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Customer's Private Information

40. BioPlus acquires, collects, and stores a massive amount of its customers' protected PII, including health information and other personally identifiable data.

41. As a condition of engaging in health-related services, BioPlus requires that these patients entrust them with highly confidential Private Information.

42. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, BioPlus assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

43. Defendant had obligations created by the Health Insurance Portability Act (42 U.S.C. § 1320d *et seq.*) ("HIPAA"), industry standards, common law, and representations made to Class Members, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

44. Defendant failed to properly safeguard Class Members' Private Information, allowing hackers to access their Private Information.

45. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant and any of its affiliates would comply with their obligation to keep such information confidential and secure from unauthorized access.

46. Prior to and during the Data Breach, Defendant promised customers that their Private Information would be kept confidential.

47. Defendant's failure to provide adequate security measures to safeguard customers' Private Information is especially egregious because Defendant operates in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to customers' highly confidential Private Information.

48. In fact, Defendant has been on notice for years that the healthcare industry and health insurance companies are a prime target for scammers because of the amount of confidential customer information maintained.

49. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[3]

[3] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warnshealthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

50. The American Medical Association ("AMA") has also warned healthcare companies about the important of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[4]

51. The number of US data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[5] In 2017, a new record high of 1,579 breaches were reported—representing a 44.7 percent increase.[6] That trend continues.

52. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[7] Indeed, when compromised, healthcare related data is among the most sensitive and

---

[4] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

[5] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), https://www.idtheftcenter.org/surveys-studys.

[6] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches/.

[7] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report*, https://www.idtheftcenter.org/2018-data-breaches/.

personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[8] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[9]

53. A 2017 study conducted by HIMSS Analytics showed that email was the most likely cause of a data breach, with 78 percent of providers stating that they experienced a healthcare ransomware or malware attack in the past 12 months.

54. Healthcare related data breaches continued to rapidly into 2021 when ReproSource was breached.[10]

55. In the Healthcare industry, the number one threat vector from a cyber security standpoint is phishing. Cybersecurity firm Proofpoint reports that "phishing is the initial point of compromise in most significant [healthcare] security incidents,

[8] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for- victims/.
[9] *Id.*
[10] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/2019-himsscybersecurity-survey.

according to a recent report from the Healthcare Information and Management Systems Society (HIMSS). And yet, 18% of healthcare organizations fail to conduct phishing tests, a finding HIMSS describes as "incredible."[11]

56. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[12]

57. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

[11] Aaron Jensen, *Healthcare Phishing Statistics: 2019 HIMSS Survey Results*, PROOFPOINT (Mar. 27, 2019), https://www.proofpoint.com/us/security-awareness/post/healthcare-phishingstatistics-2019-himss-survey-results.

[12] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

58. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . .

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it . . .

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[13]

59. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have

[13] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.

implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply the latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privilege credentials;
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise

- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**
  - use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[14]

60. These are basic, common-sense email security measures that every business, not only healthcare businesses, should be doing. BioPlus, with its heightened standard of care should be doing even more. But by adequately taking these common-sense solutions, BioPlus could have prevented this Data Breach from occurring.

61. Charged with handling sensitive PII including healthcare information, BioPlus knew, or should have known, the importance of safeguarding its customers' Private Information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on BioPlus patients as a result of a breach. BioPlus failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

62. With respect to training, BioPlus specifically failed to:

- Implement a variety of anti-ransomware training tools, in combination, such as computer-based training, classroom training, monthly newsletters, posters, login alerts, email alerts, and team-based discussions;

[14] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

- Perform regular training at defined intervals such as bi-annual training and/or monthly security updates; and
- Craft and tailor different approaches to different employees based on their base knowledge about technology and cybersecurity.

63. The PII was also maintained on BioPlus's computer system in a condition vulnerable to cyberattacks such as through the infiltration of Defendant's systems through ransomware attacks. The mechanism of the cyberattack and the potential for improper disclosure of Plaintiffs' and Class Members' PII was a known risk to BioPlus, and thus BioPlus was on notice that failing to take reasonable steps necessary to secure the PII from those risks left the PII in a vulnerable position.

C. The Monetary Value of Privacy Protections and Private Information

64. The fact that Plaintiffs' and Class Members' Private Information was stolen—and is likely presently offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

65. At all relevant times, Defendant was well aware that Private Information it collects from Plaintiffs and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

66. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of

crimes including identify theft, and medical and financial fraud.[15] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII including sensitive health information on multiple underground Internet websites, commonly referred to as the dark web.

67. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[16]

68. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[17]

---

[15] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

[16] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[17] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html [hereinafter *Web's New Hot Commodity*].

69. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[18]

70. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[19] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

71. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies

[18] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.
[19] *Web's Hot New Commodity*, *supra* note 17.

confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[20]

72. The value of Plaintiffs' and Class Members' Private Information on the black market is substantial. Sensitive health information can sell for as much as $363.[21] This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

73. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions

[20] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

[21] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/.

and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[22]

74. The ramifications of BioPlus's failure to keep its patients' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

75. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[23] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[24]

76. Breaches are particularly serious in healthcare industries. The healthcare sector reported the second largest number of breaches among all

[22] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft/.
[23] *See Medical ID Theft Checklist*, IDENTITYFORCE https://www.identityforce.com/blog/medical-id-theft-checklist-2.
[24] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches*, EXPERIAN, (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

measured sectors in 2018, with the highest rate of exposure per breach.[25] Indeed, when compromised, healthcare related data is among the most private and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[26] Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[27]

77. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

---

[25] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, (2019) https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[26] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for- victims/.

[27] *Id.*

Defendant should have particularly been aware of these risks given the significant number of data breaches affecting the medical industry and related industries.

78. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the ransomware attack into their systems and, ultimately, the theft of their customers' Private Information.

79. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[28] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[29] Based upon information and belief, the unauthorized parties utilized the

[28] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

[29] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

Private Information they obtained through the Data Breach to obtain additional information from Plaintiffs and Class Members that was misused.

80. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

81. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiffs.

82. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' Private Information has thus deprived customers of the full monetary value of their transaction with the company.

83. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breaches can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

D. BioPlus's Conduct violated HIPAA

84. HIPAA requires covered entities like BioPlus protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[30]

85. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

86. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[31]

87. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards

[30] *What is Considered Protected Health Information Under HIPAA*?, HIPPA JOURNAL, https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.
[31] *Breach Notification Rule*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

mandated by HIPAA regulations. BioPlus's security failures include, but are not limited to, the following:

- Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

- Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

- Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

- Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

- Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);

- Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

- Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. §164.306(a)(94);

- Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

- Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

- Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

88. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[32]

[32] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

89. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[33] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

90. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[34]

91. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from

[33] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'M (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.
[34] *Start with Security*, *supra* note 32.

these actions further clarify the measures businesses must take to meet their data security obligations.

92. BioPlus was at all times fully aware of its obligation to protect the Private Information of patients because of its position as a trusted healthcare provider. BioPlus was also aware of the significant repercussions that would result from its failure to do so.

E. BioPlus Failed to Comply with Healthcare Industry Standards

93. HHS's Office for Civil Rights has stated:

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry.
>
> Hackers are actively targeting healthcare organizations, as they store large quantities of highly Private and valuable data.[35]

94. HHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment, yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and

[35] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA JOURNAL (Nov. 1, 2018), https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/.

training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

95. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because the of value of the Private Information which they maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[36] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of Private Information.

96. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, BioPlus chose to ignore them. These best practices were known, or should have been known by BioPlus, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

F. Damages to Plaintiffs and the Class

97. Plaintiffs and the Class have been damaged by the compromise of their Private Information in the Data Breach.

98. The ramifications of BioPlus's failure to keep patients' Private Information secure are long lasting and severe. Once Private Information is stolen,

[36]*See, e.g., 10 Best Practices For Healthcare Security,* INFOSEC, https://resources.infosecinstitute.com/topics/healthcare-information-security/#gref.

fraudulent use of that information and damage to the victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[37]

99. In addition to their obligations under state laws and regulations, Defendant owed a common law duty to Plaintiffs and Class Members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

100. Defendant further owed and breached its duty to Plaintiffs and Class Members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

101. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiffs' and Class Members' Private Information as detailed above, and Plaintiffs are now at a heightened and increased risk of identity theft and fraud.

[37] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

102. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

103. Some of the risks associated with the loss of personal information have already manifested themselves in Plaintiffs' case. Ms. Bryan received a cryptically written notice letter from Defendant stating that her information was released, and that she should remain vigilant of fraudulent activity on her accounts, with no other explanation of where this information could have gone, or who might have access to it. Additionally, Ms. White has already been notified that her information was found on the dark web—where cybercriminals trade patient information for various illegal purposes—by her identity monitoring service.

104. Plaintiffs and the Class have suffered or face a substantial risk of suffering out-of-pocket fraud losses such as fraudulent charges on online accounts, credit card fraud, loans opened in their names, medical services billed in their name, and similar identity theft.

105. Plaintiffs and Class Members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit

report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

106. Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received services that were of a diminished value to that described in their agreements with BioPlus. They were damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and the services they received.

107. Plaintiffs and Class Members would not have obtained services from Defendant had Defendant told them that it failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from theft.

108. Plaintiffs and the Class will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

109. The theft of Social Security Numbers, which were purloined as part of the Data Breach, is particularly detrimental to victims. The U.S. Social Security Administration ("SSA") warns that "[i]dentity theft is one of the fastest growing crimes in America."[38] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use

[38] *Identity Theft And Your Social Security Number*, SOCIAL SECURITY ADMIN. (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.

the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought."[39] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[40]

110. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[41]

111. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. In the healthcare industry context, Private Information can be used to submit false insurance claims. As a result, Plaintiffs and Class Members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers, and will need to monitor their credit for an indefinite duration. For Plaintiffs and Class

[39] *Id.*
[40] *Id.*
[41] *Id.*

Members, this risk creates unending feelings of fear and annoyance. Private information is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

112. As a result of the Data Breach, Plaintiffs and Class Members' Private Information has diminished in value.

113. The Private Information belonging to Plaintiffs and Class Members is private, private in nature, and was left inadequately protected by Defendant who did not obtain Plaintiffs or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standards. Defendant disclosed information about Plaintiffs and the class that was of an extremely personal, sensitive nature as a direct result of its inadequate security measures.

114. The Data Breach was a direct and proximate result of Defendant's failure to (a) properly safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' Private

Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

115. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customer data.

116. Defendant did not properly train their employees to identify and avoid ransomware attacks.

117. Had Defendant remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiffs and Class Members' Private Information.

118. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

119. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-

nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[42]

120. Other than offering 12 or 24 months of credit monitoring, Defendant did not take any measures to assist Plaintiffs and Class Members, other than some potential ways that Plaintiffs may utilize to check their own accounts for fraud. None of these recommendations, however, require Defendant to expend any effort to protect Plaintiffs and Class Members' Private Information.

121. Defendant's failure to adequately protect Plaintiffs and Class Members' Private Information has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the incident. Instead, as BioPlus's Data Breach Notice indicates, it is putting the burden on Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

122. While Defendant offered some complimentary credit monitoring, Plaintiffs could not trust a company that had already breached their data. The credit monitoring offered from Experian does not guarantee privacy or data security for Plaintiffs who would have to expose her information once more to get monitoring

[42] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

services. Thus, to mitigate harm, Plaintiffs and Class Members are now burdened with indefinite monitoring and vigilance of their accounts.

123. Moreover, the offer of 12 months of identity monitoring to Plaintiffs and Class Members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is acquired and when it is used. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (i.e., fraudulent acquisition and use of another person's Private Information) – it does not prevent identity theft.[43] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

124. Plaintiffs and Class Members have been damaged in several other ways as well. Plaintiffs and Class Members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiffs and Class Members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. Plaintiffs and Class Members have also

[43] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

purchased credit monitoring and other identity protection services, purchased credit reports, placed credit freezes and fraud alerts on their credit reports, and spent time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiffs and Class Members also suffered a loss of the inherent value of their Private Information.

125. The Private Information stolen in the Data Breach can be misused on its own, or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to Class Members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

126. As a result of Defendant's failures to prevent the Data Breach, Plaintiffs and Class Members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

- The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;

- Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and

- Anxiety and distress resulting fear of misuse of their Private Information.

127. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

128. Plaintiffs bring this action individually and on behalf of all other persons similarly situated (the "Class") pursuant to Federal Rule of Civil Procedure 23.

129. Plaintiffs propose the following Class definition subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiffs brings this action and seeks certification of the following Class:

> All persons whose Private Information was compromised as a result of the Data Breach discovered on or about December of 2021 and who were sent notice of the Data Breach.

Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

130. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

131. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class Members would be impracticable. On information and belief, the Nationwide Class numbers in the thousands.

132. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all

members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- Whether Defendant properly implemented its purported security measures to protect Plaintiffs' and the Class's Private Information from unauthorized capture, dissemination, and misuse;
- Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;
- Whether Defendant disclosed Plaintiffs' and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;
- Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the Class's Private Information;
- Whether Defendant was negligent in failing to properly secure and protect Plaintiffs' and the Class's Private Information;
- Whether Defendant was unjustly enriched by its actions; and

- Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

133. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

134. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, all Class Members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

135. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate representatives of the Nationwide Class because their interests do not conflict with the interests of the Class they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

136. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

137. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
Negligence
(On Behalf of Plaintiffs and All Class Members)

138. Plaintiffs repeat and reallege paragraphs 1 through 127 as though fully set forth herein.

139. Upon Defendant's accepting and storing the Private Information of Plaintiffs and the Class in their computer systems and on their networks, Defendant undertook and owed a duty to Plaintiffs and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

140. Defendant owed a duty of care not to subject Plaintiffs' and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiffs and the Class were foreseeable and probable victims of any inadequate security practices.

141. Defendant owed numerous duties to Plaintiffs and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;

- to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

142. Defendant also breached their duty to Plaintiffs and Class Members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering their dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiffs' and Class Members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

143. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches within the medical industry.

144. Defendant knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class Members' Private Information.

145. Defendant breached their duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

146. Because Defendant knew that a breach of their systems would damage thousands of their customers, including Plaintiffs and Class Members, Defendant had a duty to adequately protect their data systems and the Private Information contained thereon.

147. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations including but not limited to common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

148. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

149. Defendant also had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used,

and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

150. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential Private Information.

151. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiffs' and Class member's Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

152. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

- Failing to adequately monitor the security of Defendant's networks and systems;
- Allowing unauthorized access to Class Members' Private Information;
- Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
- Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages

153. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and failure to protect Plaintiffs' and Class Members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class Members' Private Information during the time it was within Defendant's possession or control.

154. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiffs and Class Members with timely notice that their sensitive Private Information had been compromised.

155. Neither Plaintiffs nor the other Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

156. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class Members suffered damages as alleged above.

157. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class Members.

COUNT II
Breach of Contract
(On Behalf of Plaintiffs and All Class Members)

158. Plaintiffs repeat and reallege paragraphs 1 through 127 as though fully set forth herein.

159. Plaintiffs and other Class Members entered into valid and enforceable express contracts with Defendant under which Plaintiffs and other Class Members agreed to provide their Private Information to Defendant, and Defendant agreed to provide testing services and, impliedly, if not explicitly, agreed to protect Plaintiffs and Class Members' Private Information.

160. These contracts include HIPAA privacy notices and explanation of benefits documents.

161. To the extent Defendant's obligation to protect Plaintiffs' and other Class Members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and other Class Members' Private Information, including in accordance with HIPAA regulations; federal, state and local laws; and industry standards. No Plaintiffs would have entered into these contracts with Defendant without understanding that Plaintiffs' and other Class Members' Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

162. A meeting of the minds occurred, as Plaintiffs and other Class Members agreed, among other things, to provide their Private Information in exchange for Defendant's agreement to protect the confidentiality of that Private Information.

163. The protection of Plaintiffs and Class Members' Private Information were material aspects of Plaintiffs' and Class Members' contracts with Defendant.

164. Defendant's promises and representations described above relating to HIPAA and industry practices, and about Defendant' purported concern about their clients' privacy rights became terms of the contracts between Defendant and their

clients, including Plaintiffs and other Class Members. Defendant breached these promises by failing to comply with HIPAA and reasonable industry practices.

165. Plaintiffs and Class Members read, reviewed, and/or relied on statements made by or provided by BioPlus and/or otherwise understood that BioPlus would protect its patients' Private Information if that information were provided to BioPlus.

166. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

167. As a result of Defendant's breach of these terms, Plaintiffs and other Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the secure health services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial and medical accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and Plaintiffs and other Class Members have been put at increased risk of future identity theft,

fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

168. Plaintiffs and Class Members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and All Class Members, in the Alternative to Count II)

169. Plaintiffs repeat and reallege paragraphs 1 through 127 as though fully set forth herein.

170. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the provision of healthcare services, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

171. Specifically, Plaintiffs entered into a valid and enforceable implied contract with Defendant when she first entered into the testing services agreement with Defendant.

172. The valid and enforceable implied contracts to provide pharmacy services that Plaintiffs and Class Members entered into with Defendant include

Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant creates on its own from disclosure.

173. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

174. Defendant solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

175. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

176. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

177. Under implied contracts, Defendant and/or its affiliated providers promised and were obligated to: (a) provide pharmacy services to Plaintiffs and Class Members; and (b) protect Plaintiffs' and the Class Members' Private Information provided to obtain such benefits of such services. In exchange, Plaintiffs

and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

178. Both the provision of testing services and the protection of Plaintiffs' and Class Members' Private Information were material aspects of these implied contracts.

179. The implied contracts for the provision of pharmacy services—contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Data Breach notification letter.

180. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs and protect the privacy of Plaintiffs' and Class Members Private Information.

181. Consumers of pharmacy services value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining such services. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be

safeguarded and protected, or entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

182. A meeting of the minds occurred, as Plaintiffs and Class Members agreed and provided their Private Information to Defendant and/or its affiliated healthcare providers, and paid for the provided testing services in exchange for, amongst other things, both the provision of healthcare and the protection of their Private Information.

183. Plaintiffs and Class Members performed their obligations under the contract when they paid for Defendant's services and provided their Private Information.

184. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by the Data Breach.

185. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiffs' and Class Members Private Information as evidenced by its notifications of the Data Breach to Plaintiffs and Class Members. Specifically, Defendant did not comply with industry standards,

standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiffs' and Class Members private information as set forth above.

186. The Data Breach was a reasonably foreseeable consequence of Defendant's action in breach of these contracts.

187. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

188. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated providers.

189. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care

and treatment, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

190. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

191. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and All Class Members)

192. Plaintiffs repeat and reallege paragraphs 1 through 127 as though fully set forth herein.

193. In providing their Private Information to Defendant, Plaintiffs and Class Members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiffs and Class Members to safeguard and keep confidential that Private Information.

194. Defendant accepted the special confidence Plaintiffs and Class Members placed in it, as evidenced by its assertion that it is "committed to protecting

the privacy of [Plaintiffs'] personal information" as included in the Data Breach notification letter.

195. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became a guardian of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiffs and Class Members for the safeguarding of Plaintiffs' and class member's Private Information.

196. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its customer's relationship, in particular, to keep secure the Private Information of its customers.

197. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to protect the integrity of the systems containing Plaintiffs' and class member's Private Information.

198. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

199. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise,

publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Cyber-Attack and Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Cyber-Attack and Data Breach for the remainder of the lives of Plaintiffs and class members; and (vii) the diminished value of Defendant's services they received.

200. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
Violation of Florida's Deceptive and Unfair Trade Practices Act
Fla. Stat. § 501.201, *et seq.*
(On Behalf of Plaintiffs and Class Members)

201. Plaintiffs repeat and reallege paragraphs 1 through 127 as though fully set forth herein.

202. Plaintiffs, Class Members, and Defendant each qualify as a person engaged in trade or commerce as contemplated by the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA") Fla. Stat. § 501.201, *et seq.*

203. As alleged herein in this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of FDUTPA, including but not limited to:

a. representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

c. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private

Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Cyber-Attack and data breach;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

204. Defendant's representations and omissions were material because it was likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

205. In addition, Defendant's failure to secure consumers' PHI violated the FTCA and therefore violated FDUTPA.

206. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiffs and Class

Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

207. The aforesaid conduct constitutes a violation of FDUTPA, Fla. Stat. § 501.204, in that it is a restraint on trade or commerce.

208. The Defendant's violations of FDUTPA have an impact of great and general importance on the public, including Floridians. Thousands of Floridians have used BioPlus Specialty Pharmacy's services, many of whom have been impacted by the Data Breach. In addition, Florida residents have a strong interest in regulating the conduct of its corporate citizens such as BioPlus, whose policies and practices described herein affected millions across the country.

209. As a direct and proximate result of Defendant's violation of FDUTPA, Plaintiffs and Class Members are entitled to a judgment under Fla. Stat. § 501.201, *et seq*, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorney's fees), and such other further relief as the Court deems just and proper.

210. Defendant's implied and express representations that it would adequately safeguard Plaintiffs' and other Class Members' Private Information constitute representations as to characteristics, uses or benefits of services that such services did not actually have, in violation of Fla. Stat. § 501.202(2).

211. On information and belief, BioPlus formulated and conceived of the systems it used to compile and maintain patient information largely within the state of Florida, oversaw its data privacy program complained of herein from Florida, and its communications and other efforts to hold patient data largely emanated from Florida.

212. Most, if not all, of the alleged misrepresentations and omissions by BioPlus complained of herein that led to inadequate safety measures to protect patient information occurred within or were approved within Florida.

213. Defendant's implied and express representations that it would adequately safeguard Plaintiff's and Class Members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of Fla. Stat. § 501.204.

214. Defendant knowingly made false or misleading statements in its privacy policy regarding the use of personal information submitted by members of the public in that Defendant advertised it is committed to protecting privacy and securely maintaining personal information. Defendant did not securely maintain personal information as represented, in violation of Fla. Stat. § 501.171.

215. These violations have caused financial injury to Plaintiff and Class Members and have created an unreasonable, imminent risk of future injury.

216. Accordingly, Plaintiffs, on behalf of themselves and the other Class Members, bring this action under the Deceptive and Unfair Trade Practices Act to seek such injunctive relief necessary to enjoin further violations and to recover costs of this action, including reasonable attorneys' fees and costs.

COUNT VI
Violation of New Jersey's Consumer Fraud Act
N.J. Rev. Stat. § 56:8-1, *et seq.*
(On Behalf of Plaintiffs and Class Members)

217. Plaintiffs repeat and reallege paragraphs 1 through 127 as though fully set forth herein.

218. Plaintiffs, Class Members, and Defendant each qualify as a person engaged in trade or commerce as contemplated by New Jersey's Consumer Fraud Act, N.J. Rev. Stat. § 56:8-1, *et seq* ("CFA").

219. As alleged herein in this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of the CFA, including but not limited to:

h. representing that its services were of a particular standard or quality that it knew or should have known were of another;

i. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

j. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

k. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Cyber-Attack and data breach;

l. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

m. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Private Information; and

n. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Personal Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

220. Defendant's representations and omissions were material because it was likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

221. In addition, Defendant's failure to secure consumers' PHI violated the FTCA and therefore violates the CFA.

222. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiffs and Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

223. The aforesaid conduct constitutes a violation of the CFA, in that it is a restraint on trade or commerce.

224. The Defendant's violations of the CFA have an impact of great and general importance on the public, including New Jerseyans. Thousands of New Jerseyans have used BioPlus Specialty Pharmacy's services, many of whom have been impacted by the Data Breach. In addition, New Jersey residents have a strong interest in regulating the conduct of corporations that do business within the state's such as BioPlus, whose policies and practices described herein affected millions across the country.

225. As a direct and proximate result of Defendant's violation of the CFA, Plaintiffs and Class Members are entitled to a judgment under N.J. Rev. Stat. § 56:8-

1, *et seq*, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorney's fees), and such other further relief as the Court deems just and proper.

226. Defendant's implied and express representations that it would adequately safeguard Plaintiff's and other Class Members' Private Information constitute representations as to characteristics, uses or benefits of services that such services did not actually have, in violation of the CFA.

227. Defendant's implied and express representations that it would adequately safeguard Plaintiff's and Class Members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of the CFA.

228. Defendant knowingly made false or misleading statements in its privacy policy regarding the use of personal information submitted by members of the public in that Defendant advertised it is committed to protecting privacy and securely maintaining personal information. Defendant did not securely maintain personal information as represented, in violation of the CFA. N.J. Rev. Stat. § 56:8-196.

229. Further, BioPlus inexplicably waited nearly one month before it began sending notification letters to customers of the data breach incident. This delay

resulted in additional harms to customers who were not notified that their data was lost until over 30 days after the incident, leaving the information exposed and vulnerable to misuse without customers' knowledge, a violation of N.J. Rev. Stat. § 56:8-163.

230. These violations have caused financial injury to Plaintiffs and Class Members and have created an unreasonable, imminent risk of future injury.

231. Accordingly, Plaintiffs, on behalf of themselves and the other Class Members, bring this action under the Consumer Fraud Act to seek such injunctive relief necessary to enjoin further violations and to recover costs of this action, including reasonable attorneys' fees and costs.

COUNT VII
Violation of the Connecticut Unfair Trade Practices Act
Con. Gen, Stat. §42-110, *et seq.*
(On Behalf of Plaintiffs and Class Members)

232. Plaintiffs repeat and reallege paragraphs 1 through 127 as though fully set forth herein.

233. Plaintiffs, Class Members, and Defendant each qualify as a person engaged in trade or commerce as contemplated by the Connecticut Unfair Trade Practices Act. Con. Gen, Stat. §42-110(a) ("CUTPA").

234. As alleged herein in this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of the CUTPA, including but not limited to:

a. representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

c. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Cyber-Attack and data breach;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security

and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

235. Defendant's representations and omissions were material because it was likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

236. In addition, Defendant's failure to secure consumers' PHI violated the FTCA and therefore violates the CUTPA.

237. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiffs and Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

238. The aforesaid conduct constitutes a violation of the CUTPA, Con. Gen, Stat. §42-110 *et seq.*, in that it is a restraint on trade or commerce.

239. The Defendant's violations of the CUTPA have an impact of great and general importance on the public, including people from Connecticut. Thousands of Connecticuters have used BioPlus Specialty Pharmacy's services, many of whom have been impacted by the Data Breach. In addition, Connecticut residents have a strong interest in regulating the conduct of its corporate citizens such as BioPlus, whose policies and practices described herein affected millions across the country.

240. As a direct and proximate result of Defendant's violation of the CUTPA, Plaintiffs and Class Members are entitled to a judgment under Con. Gen, Stat. §42-110 *et seq.*, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorney's fees), and such other further relief as the Court deems just and proper.

241. Defendant's implied and express representations that it would adequately safeguard Plaintiffs' and other Class Members' Private Information constitute representations as to characteristics, uses or benefits of services that such services did not actually have, in violation of Con. Gen, Stat. §42-110(a).

242. Defendant's implied and express representations that it would adequately safeguard Plaintiffs' and Class Members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of Con. Gen, Stat. §42-110(a).

243. Defendant knowingly made false or misleading statements in its privacy policy regarding the use of personal information submitted by members of the public in that Defendant advertised it is committed to protecting privacy and securely maintaining personal information. Defendant did not securely maintain personal information as represented, in violation of Con. Gen, Stat. §42-110(a).

244. These violations have caused financial injury to Plaintiffs and Class Members and have created an unreasonable, imminent risk of future injury.

245. Accordingly, Plaintiffs, on behalf of themselves and the other Class Members, bring this action under the CUTPA to seek such injunctive relief necessary to enjoin further violations and to recover costs of this action, including reasonable attorneys' fees and costs.

COUNT VIII
Declaratory Relief
(On Behalf of Plaintiffs and All Class Members)

246. Plaintiffs repeat and reallege paragraphs 1 through 127 as though fully set forth herein.

247. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

248. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information.

Plaintiffs and the Class remain at imminent risk that further compromises of their PII will occur in the future.

249. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

250. Defendant still possesses the PII of Plaintiffs and the Class.

251. Defendant has made no announcement that it has changed its data storage or security practices relating to the PII.

252. Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

253. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at BioPlus. The risk of another such breach is real, immediate, and substantial.

254. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at BioPlus, Plaintiffs and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by

employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

255. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at BioPlus, thus eliminating the additional injuries that would result to Plaintiffs and Class Members, along with other consumers whose PII would be further compromised.

256. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that BioPlus implement and maintain reasonable security measures, including but not limited to the following:

- Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on BioPlus's systems on a periodic basis, and ordering BioPlus to promptly correct any problems or issues detected by such third-party security auditors;
- engaging third-party security auditors and internal personnel to run automated security monitoring;
- auditing, testing, and training its security personnel regarding any new or modified procedures;

- purging, deleting, and destroying Private Infomration not necessary for its provisions of services in a reasonably secure manner;
- conducting regular database scans and security checks; and
- routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For declaratory relief concluding that that BioPlus owed, and continues to owe, a legal duty to employ reasonable data security to secure the Sensitive Information with which it is entrusted, specifically including

information pertaining to healthcare and financial records it obtains from its clients, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

D. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. Ordering Defendant to pay for not less than three (3) years of credit monitoring services for Plaintiffs and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

Dated: January 5, 2022

Respectfully Submitted,

By: *Scott D. Hirsch*
Scott David Hirsch
SCOTT HIRSCH LAW GROUP PLLC
Fla. Bar No. 50833
6810 N. State Road 7
Coconut Creek, FL 33073
Tel: (561) 569-7062
Email: scott@scotthirschlawgroup.com

Nicholas A. Migliaccio (*pro hac vice* forthcoming)
Jason S. Rathod (*pro hac vice* forthcoming)
MIGLIACCIO & RATHOD LLP
412 H Street NE
Washington, DC 20002
Tel: (202) 470-3520
Email: nmigliaccio@classlawdc.com
Email: jrathod@classlawdc.com